Electronic data storage and display apparatus

This invention relates to electronic data storage and display apparatus, and in particular to such apparatus for the storage and display of electronic data that has commercial value such as electronically formatted books.

With the advances in the fields of microchip and display screen technologies, and allied computing advances it is becoming increasingly economically viable to produce apparatus that is easily portable and can store, manipulate and display large quantities of electronic data. There is, however, often a reluctance on the part of the owners of that data to release it to members of the public because of the ease of replication of electronic data. For data with commercial value such replication deprives the parties involved with the genesis and distribution of the data of a suitable reward for the production or distribution of that data. For example, if the data when rendered legible by suitable software is the text of a book, then if the data becomes available to the public not under the control of a distributor, copyright owner or the like, then if electronic copies of that data may easily be made, the publisher of that data and possibly others will suffer economic damage, for example being able only to sell fewer copies of a book than would otherwise be the case.

One approach is to render the data "copy-protected". This can be effective in some environments, though there is a widespread belief that copy-protection systems simply pose a challenge to those who would circumvent them. However, copy-protection systems which rely on encryption and decryption of data provide some effectiveness, for example as described in WO 97/44736. However, the system is cumbersome and not always user-

friendly. Systems which have been proposed for use in this area include those described in EP-A-0665486, WO 95/08231, WO 98/08344 and WO99/12087, though the last of these does not form part of the state of the art. All seek to enhance the security against copying by using cryptographic techniques and generally require the use of encryption/decryption keys which are transmitted, after an authenticated request has been received, e.g. over a suitable communications link which has been established for that purpose.

The present invention provides apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port,and wherein the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and characterised in that the apparatus is configured such that one encryption key references addresses in a portion of Read Only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

This approach, especially when used on a direct communications channel between user and information provider, rather than via a wide area network such as the internet, is advantageous as there is never any need to engage in a key request dialogue. Instead, an encryption/decryption key may be generated and used by reference to the addresses of resident code areas in ROM in the apparatus. This is explained in more detail below.

In use, for example when the user of the apparatus wishes to obtain an electronic version of a book, the user connects the apparatus of the present invention to an appropriate source of electronic data in the following manner:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

By having the apparatus and the data source interact in this fashion, the electronic data is encrypted when it is travelling between the owners or distributors of the data and the legitimate end user of the data. Because the encryption key between the data source and the apparatus is altered after each transaction, it will be very difficult for an illegitimate receiver of the data to decrypt that data. Even if that does prove possible,

the illegitimate receiver only then gains the encryption key for one specific piece of apparatus the next time it connects to the data source and not the data source as a whole.

In a particularly preferred embodiment of the present invention the apparatus stores two encryption keys, one of which is stored in either Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory, and the other of which is stored in Read Only Memory. The encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is the key that is rewritten when the apparatus interacts with a data store.

In a preferred embodiment of the present invention, the encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is 16 bytes in size. The portion of Read Only Memory, the content of which is used to encrypt/decrypt transmitted/received data, is preferably 256 bytes in size.

The data storage means in the apparatus of the present invention is preferably non-volatile random access memory. It may, however, alternatively be in the form of a magnetic disk, built into the casing and so constructed that attempts to remove the disc would result in the destruction of at least the data on the disc, or any other known data storage media which could be built into the casing.

The method of communication between the apparatus of the present invention and the data store is most preferably via the telephone network, and at least one input/output port in the casing is adapted to connect to that network most preferably via an electromagnetic radiation link.

In alternative embodiments other methods of connection the data source are possible and at least one input/output port in the casing is appropriately configured for that connection.

In a preferred embodiment of the present invention, the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form. The computer hardware preferably includes user control means which will allow a user of the apparatus to move through the data in an appropriate fashion. The display screen of the present invention is preferably of sufficient size that the viewing area thereof is at least 110mm by 180mm. The screen is preferably of a type that has a low power consumption.

In an alternative embodiment of the present invention, the apparatus additionally includes known means for the generation of sound. The sound generation means can be controlled by the computer software that controls the display means, or by independent control means. In this embodiment the reader of, for example, a book about ornithology may be played the sound of the bird which he is reading about.

It will be appreciated that the size of the data storage means in the apparatus of the present invention will be finite. As such, and to avoid the problem of either having to delete and loose a previously acquired set of data, or having to acquire a new apparatus, the apparatus of the present invention is configured so that it can export some or all of the data stored in the data storage means. To prevent duplicatable and readable copies of the data being exported, the apparatus is configured only to export the data in an encrypted form.

It is clearly desirable that the exported data can be imported back onto the apparatus of the present invention, so that the data can be viewed again at a later date.

The data is preferably exported to and imported from a dedicated data store adapted to interact with the apparatus of the present invention. In the first preferred embodiment, the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

In a second preferred embodiment the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

In this second embodiment the data store stores the data in encrypted form. Preferably there is, however, a little un-encrypted data attached to the encrypted data. That un-encrypted data can, for example, give an indication of the contents of the data, and/or the apparatus that placed the data in the data store and consequently the apparatus that can decrypt the data. This will allow more than one piece of apparatus of the present invention to use the data store.

In either of the two above described embodiments, the data transfer between the apparatus and the data store can be either via electrical or optical cables or via electromagnetic radiation.

The apparatus of the present invention may be provided with its own power source and/or means for taking power from an external power source.

In one particularly preferred embodiment of the present invention, the apparatus is provided with a computer chip that has the specification, details and method of operation as follows:

SPECIFICATION

EEPROM: 16 bytes of key memory (addresses 0 - 15).
112 bytes of user memory (addresses 16 - 127).

POWER: 5mA @5V when active
6mA @5V when writing to eeprom
10uA @5V in power saving mode.

CONVERSION RATE: approx. 30KPS.

MASK LOOKUP TABLE

Rom address

0 = 255
1 = 254
2 = 253
3 = 252
4 = 251
5 = 250
. . . . . .
. . . . . .
. . . . . .
250 = 5
251 = 4
252 = 3
253 = 2
254 = 1
255 = 0

starting with address 0 = 255 the rom table is filled by the following formula :

rom table[address] = 255 - address

ENCRYPTION/DECRYPTION OPERATION

Version 1.0 of crypto uses a key length of 16 bytes.

First write the 16 byte key to eeprom addresses 0 - 15.
Each byte of key is used to access an 8 bit mask from within a 256 byte lookup table.
Each data byte is encrypted/decrypted by exclusive oring it with the 8 bit mask.
As each byte of data is encrypted/decrypted the mask is rotated one bit position to the left.
After eight bit rotations a new mask is loaded using the next key in the sequence of sixteen.
The sequence of masks will be repeated again when all sixteen have been used.

OPERATION MODES

EEPROM WRITE (mode 0)

1. Wait until BUSY line is a logic low.
2. Write number 0 (binary 00000000) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT1.
5. Wait until BUSY line is a logic low.
6. Write eeprom data to PORT2.

Steps 1 & 2 need only be done once to set eeprom write mode.

DECRYPT DATA (mode 1)

1. Wait until BUSY line is a logic low.
2. Write number 1 (binary 00000001) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for decryption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read decrypted data from PORT3.

Steps 1 & 2 need only be done once to set data decrypt mode.

ENCRYPT DATA (mode 2)

1. Wait until BUSY line is a logic low.
2. Write number 2 (binary 00000010) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for encyption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read encrypted data from PORT3.

Steps 1 & 2 need only be done once to set data encrypt mode.

EEPROM READ (mode 3)

1. Wait until BUSY line is a logic low.
2. Write number 3 (binary 00000011) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT2.
5. Wait until BUSY line is a logic low.
6. Read eeprom data from PORT3.

Steps 1 & 2 need only be done once to set eeprom read mode.

RESET COUNTERS (mode 4)

This will reset the rotate counter & key index to zero.

1. Wait until BUSY line is a logic low.
2. Write number 4 (binary 00000100) to PORT0.

POWER SAVING (mode 5)

This will put the crypto pcb into sleep mode.

1. Wait until BUSY line is a logic low.
2. Write number 5 (binary 00000101) to PORT0.
3. Wait until BUSY line is a logic zero before proceeding.

Waking up the crypto unit from power saving mode

1. Do a dummy read from PORT0 or Write a new operation mode to PORT0.
2. Wait until BUSY line is a logic low before proceeding.

20 WAY IDC CONNECTOR PIN OUT & DESCRIPTION

1.	GND	Power supply 0V connection.
2.	+5/3.3 VDC	Power supply positive connection.
3.	\RESET	Active low external chip reset. Leave disconnected if control of reset is not required. The chip takes approximately 80mS to reset after a low to high transition of the reset pin.
4.	\RD	Active low read control input.
5.	\WR	Active low write control input
6.	\CS	Active low chip select input.
7.	A0	Port address select input.
8.	A1	Port address select input.
9.	D7	Bit 7 of bi-directional data bus.
10.	D6	Bit 6 of bi-directional data bus.
11.	D5	Bit 5 of bi-directional data bus.
12.	D4	Bit 4 of bi-directional data bus.
13.	D3	Bit 3 of bi-directional data bus.
14.	D2	Bit 2 of bi-directional data bus.
15.	D1	Bit 1 of bi-directional data bus.
16.	D0	Bit 0 of bi-directional data bus.
17.	BUSY	Active high busy output.
18.	\BUSY	Active low busy output.
19.	RxD	Serial data input (do not connect).
20.	TxD	Serial data output (do not connect).